FAA National Software Conference, June 2001
Safety & Security Aspects of SW Assurance

Safety and Security Aspects of Software Assurance

Warren Naylor, BAE Systems SETA II Support to:
FAA, Office of Information Services
Process Engineering Division, AIO-200
Software Safety and Certification
PH. (202) 548-5575
warren.naylor@baesystems.com

FAA Mission Goals*

- Safety:
  - By 2007, reduce U.S. aviation accident rates by 80 percent from 1996 levels.
- Security:
  - Securing the ATC (NAS) computer systems that provide information to controllers and flight crew is critical to the safe and expeditious movement of aircraft.

** FAA Office of Information Security Program Management Plan; August 29 2000*

Safety and Security Definitions:

- Safety is freedom from those conditions that can cause death, injury, occupational illness, damage to or loss of equipment or property or damage to the environment.
- Security is the prevention of advertent conditions that can compromise FAA sensitive data or information that could potentially lead to accidents

3

NAS Software Safety Strategies*

- Error prevention through design assurance that could potentially lead to accidents
- Safety information sharing and analysis
- Approval and lifecycle monitoring

* *FAA Achievement Plan: FAA Corporate Projects, FY 2000-2002 and Beyond*

4

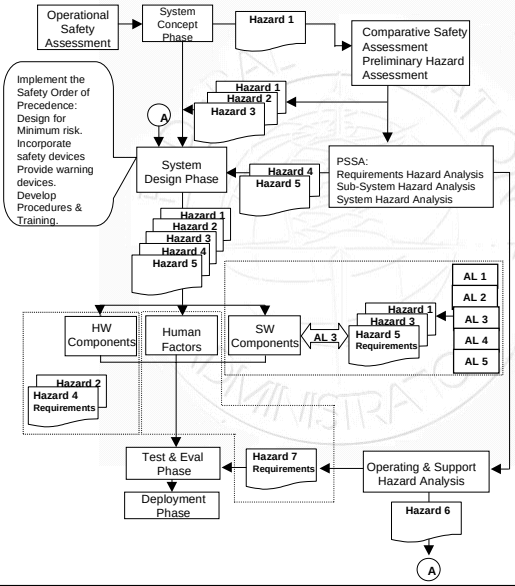
Information Security Strategies*

- *Implementing an ISS Framework that consists of:
  - A structural,
  - Operational, and
  - Process models

** FAA Office of Information Security Program Management Plan; August 29 2000*

5

Simplified Iterative Safety Model

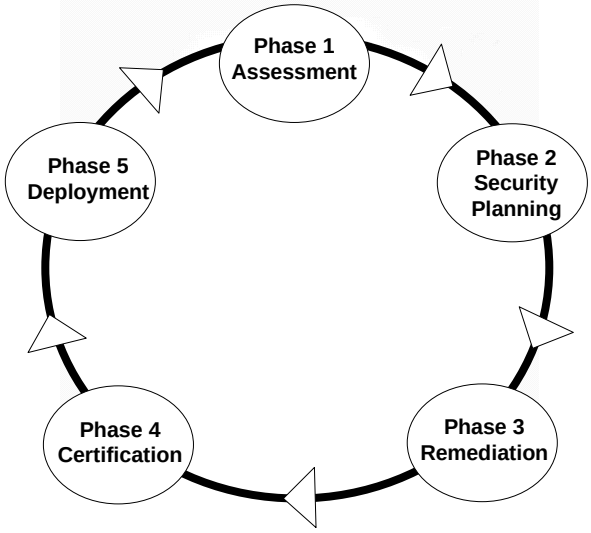


Note:

A hazard is the potential for harm. A hazard is not an accident, although if not adequately mitigated could result in an accident.

6

Simplified Iterative Security Model



7

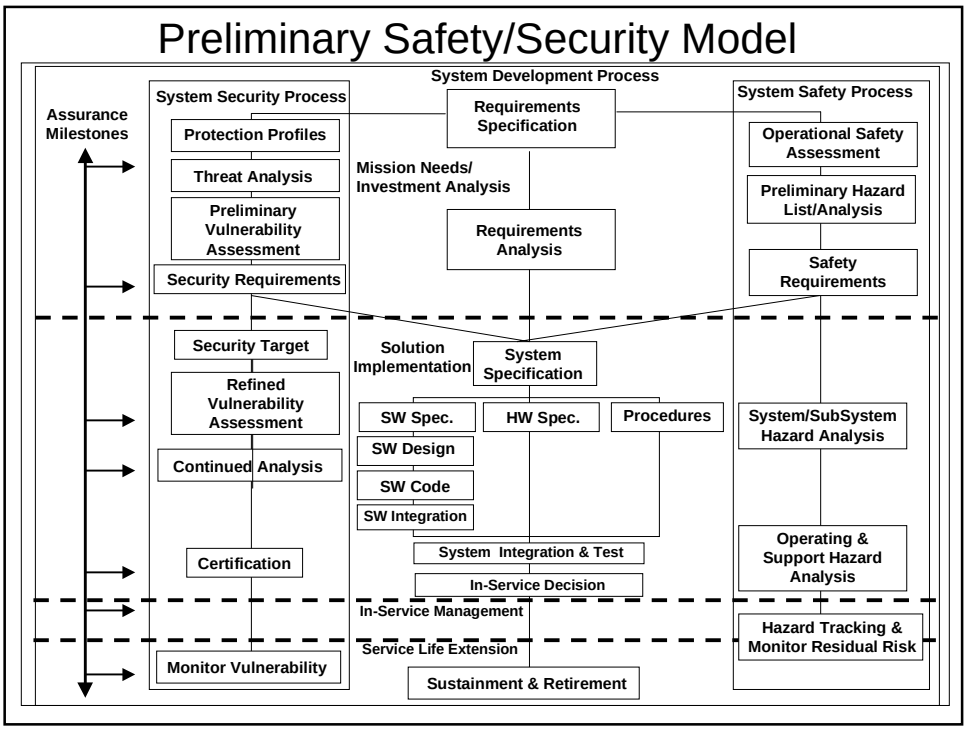
Safety and Security Similarities

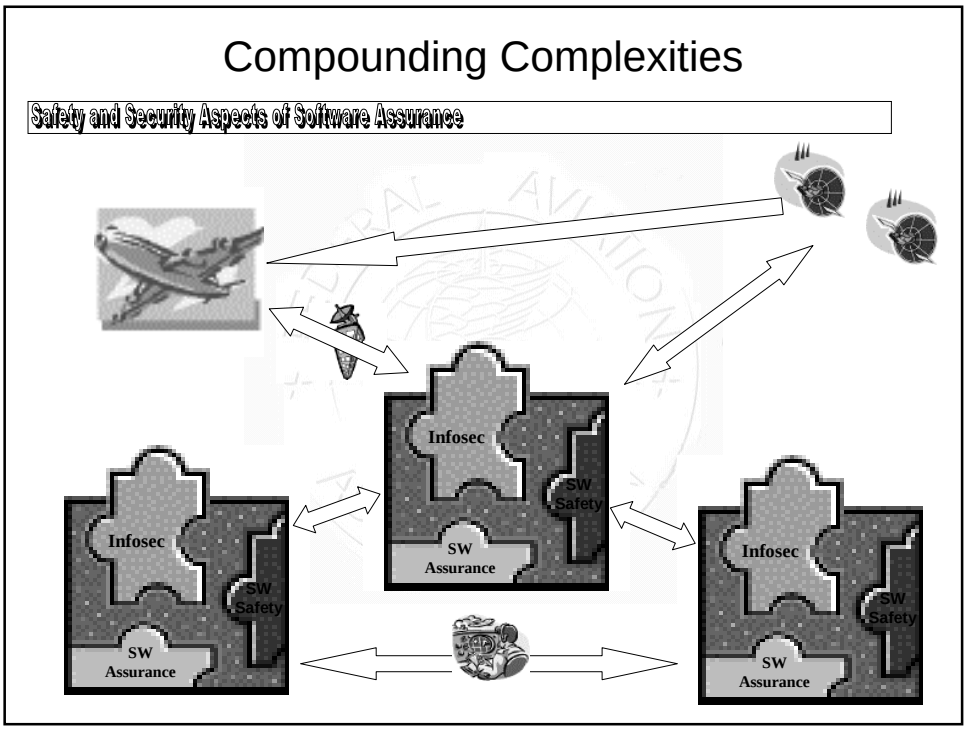
ANALYSIS → **REQUIREMENTS** → **VERIFICATION**

SECURITY	? =	SAFETY
• Vulnerability/Threat Assessment • Risk Determination • Security Requirements • Penetration testing		• Operational Safety Assessment • Risk Determination • Safety Requirements • Requirements-based testing

8

FAA National Software Conference, June 2001
Safety & Security Aspects of SW Assurance

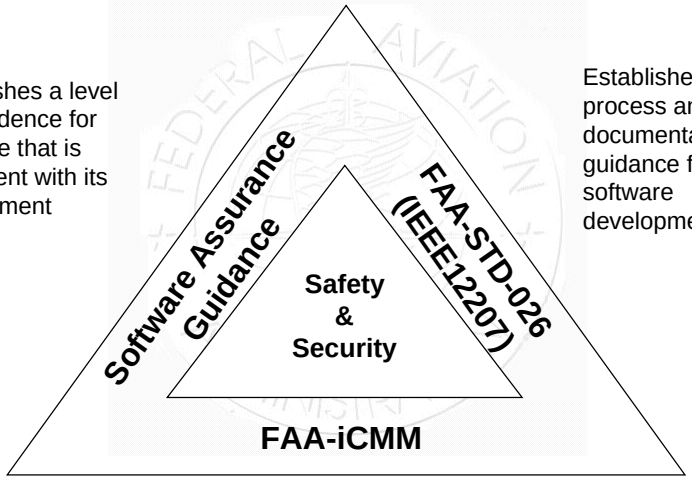




FAA National Software Conference, June 2001
Safety & Security Aspects of SW Assurance

Software Quality Triangle

Establishes a level of confidence for software that is consistent with its environment



Establishes a process and documentation guidance for software development

Establishes essential elements of an organizations software acquisition, engineering, and management process

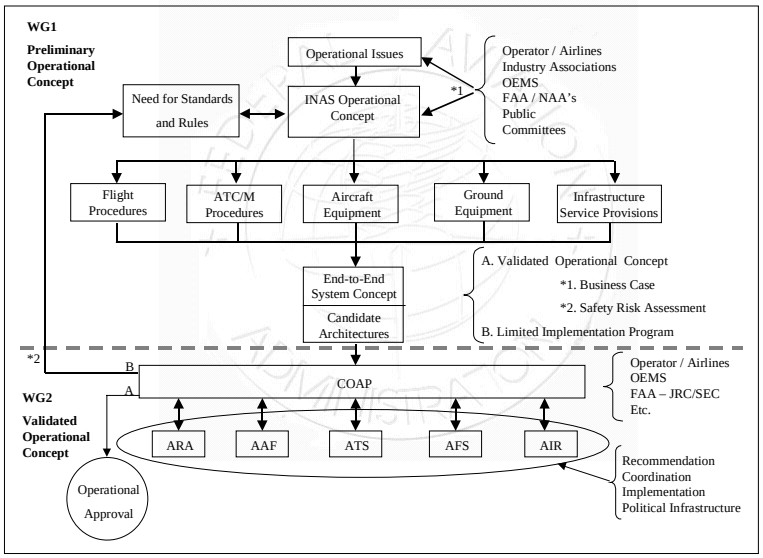
11

Cooperative Operational Approval Council

- A process to ensure adequate coordination and communication among stakeholders to ensure timely implementation of an operational capability
- Implemented through an independently recognized coordinating body
- Establish an approval basis and plan for implementation
- Ensure evidence of completion of required steps
- Ensure compliance with approval basis

12

Proposed NAS COAP Concept



13

Roles of Coordinating Council

- Formal avenue for addressing safety, security and human factors issues
- Ensure airborne equipage and ground infrastructure investments are consistent and matched to achieve operational benefits
- Ensure shared and proper mitigation of operational hazards and risk mitigation strategies

14

Responsibilities of Coordinating Council

- Assure a commonly agreed operational concept is validated
- Assure proper designation of approval authority for each element within the integrated system
- Assure there is evidence of approval of the products and process documentation
- Serve as approval authority and acceptor of residual risk

15

System Engineering Council

- Purpose
  - Orchestrates common systems engineering activities across the NAS
  - Responsibility, authority, and accountability for the development, documentation, deployment, control, and monitoring of the systems engineering process.
- Products
  - System Engineering Management Plan
  - System Engineering Manual

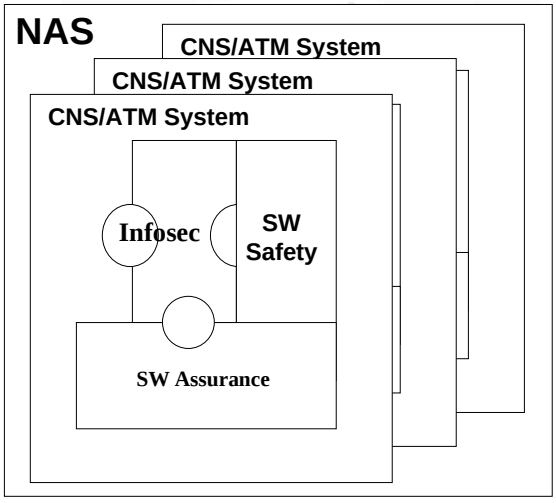
16

System Safety Working Group

- Purpose
  - Working arm of the System Engineering Council
  - Assists in supporting and evaluating Comparative and Operational Safety Assessments
  - Analyzes NAS System Level Hazards and provides mitigation assistance to the various business units
- Products
  - System Safety Management Plan
  - System Safety Handbook
  - Applicable Hazard Analyses

17

Objective : Enhanced Safety !



18

Summary

- The FAA continues to refine its systems and software engineering processes
- We are focusing on the technical and programmatic efficiencies that can be achieved by integrating safety and security into the system life cycle processes.

19

Benefits of Refining NAS SW Assurance Efforts

- ✓Reduction of wasteful false starts
- ✓Reduced costs
- ✓More timely completion of needed changes
- ✓Improved coordination with internal and external stakeholders
- ✓Building safer and more secure systems

20

Any Questions ?

Backup slides

Universal Safety/Security Order of Precedence

- ✓ **Design for Minimum Risk**. The system design will seek to eliminate hazards. If an identified hazard cannot be eliminated, the associated risk will be reduced to an acceptable level through design selection.
- ✓ **Incorporate Safety Devices**. When identified hazards cannot be eliminated or their associated risk adequately reduced through design selection, that risk will be reduced to an acceptable level through the use of fixed, automatic, or other protective safety design features or devices.
- ✓ **Provide Warning Devices**. Warning devices may be utilized to augment or reduce the probability of a hazard occurrence when neither design or safety devices effectively eliminate or reduce the associated risk to an acceptable level. Warning signals and their application shall be succinct and easily understood to reduce the risk of misinterpretation and shall be standardized to be consistent with other like systems.
- ✓ **Develop Procedures and Training**. When risk reduction is not adequately achieved through design, safety devices, and/or through warnings, then training and implementation of procedures and training are utilized.

23

Acronyms (1/2)

- AMS Acquisition Management System
- CRA Comparative Risk Analysis
- FAA Federal Aviation Administration
- FMEA Failure Modes Effects Analysis
- HTRR Hazard Tracking and Risk Resolution
- ICAO International Civil Aviation Organization
- ISD In-service Decision
- JRC Joint Resource Council
- LMS Life-cycle Management System
- NAS National Airspace System

24

Acronyms (2/2)

Safety and Security Aspects of Software Assurance

• OSA	Operational Safety Assessment
• PHA	Preliminary Hazard Assessment
• SEMP Plan	System Engineering Management
• SEM	System Engineering Manual
• SHA	System Hazard Analysis
• SSH	System Safety Handbook
• SSHA	SubSystem Hazard Analysis
• SSMP	System Safety Management Plan
• SSAR	System Safety Assessment Report

25